IT & C

ISSN 2821 - 8469, ISSN – L 2821 - 8469, Volumul 2, Numărul 2, Iunie 2023

Mecanismele de consens blockchain

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Mecanismele de consens blockchain, *IT & C*, **2**:2, 26-32, DOI: 10.58679/IT78749, https://www.internetmobile.ro/mecanismele-de-consens-blockchain/

Publicat online: 09.04.2023

Mecanismele de consens blockchain

Nicolae Sfetcu
nicolae@sfetcu.com

Blockchain consensus mechanisms

Abstract

In principle, any node within a blockchain network can propose adding new information to the blockchain. To validate that this addition of information (eg a transaction record) is legitimate, the nodes must reach some form of agreement. This is where a "consensus mechanism" comes into play. In short, a consensus mechanism is a predefined specific (cryptographic) validation method that ensures correct sequencing of transactions on the blockchain. In the case of cryptocurrencies, such sequencing is necessary to address the problem of "double spending" (ie the problem that the same payment instrument or asset can be transferred multiple times if the transfers are not centrally recorded and controlled.

Keywords: blockchain technology, blockchain, philosophy, consensus mechanisms, proof of work, proof of stake

Rezumat

În principiu, orice nod din cadrul unei rețele blockchain poate propune adăugarea de informații noi în blockchain. Pentru a valida dacă această adăugare de informații (de exemplu o înregistrare de tranzacție) este legitimă, nodurile trebuie să ajungă la o formă de acord. Aici intră în joc un „mecanism de consens”. Pe scurt, un mecanism de consens este o metodă de validare specifică (criptografică) predefinită care asigură o secvențiere corectă a tranzacțiilor pe blockchain. În cazul criptomonedelor, o astfel de secvențiere este necesară pentru a aborda problema „dublei cheltuieli” (adică problema că același instrument de plată sau activ poate fi transferat de mai multe ori dacă transferurile nu sunt înregistrate și controlate centralizat.

Cuvinte cheie: tehnologia blockchain, blockchain, mecanisme de consens, proof of work, proof of stake

IT & C, Volumul 2, Numărul 2, Iunie 2023, pp. 26-32
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT78749
URL: https://www.internetmobile.ro/mecanismele-de-consens-blockchain/

Introducere

În termeni simpli, blockchain poate fi gândit ca o bază de date distribuită. Adăugările la această bază de date sunt inițiate de unul dintre membri (adică nodurile de rețea), care creează un nou „bloc” de date, care poate conține tot felul de informații. Acest nou bloc este apoi transmis tuturor părților din rețea într-o formă criptată (utilizând criptografie), astfel încât detaliile tranzacției să nu fie făcute publice. (1) Cei din rețea (adică celelalte noduri de rețea) determină în mod colectiv validitatea blocului în conformitate cu o metodă de validare algoritmică predefinită, denumită în mod obișnuit „mecanism de consens” (2). Odată validat, noul „bloc” este adăugat la blockchain, ceea ce duce în esență la o actualizare a registrului tranzacției care este distribuit în rețea. (3)

În principiu, acest mecanism poate fi utilizat pentru orice tip de tranzacție de valoare și poate fi aplicat oricărui activ care poate fi reprezentat într-o formă digitală (4).

Fiecare utilizator dintr-o rețea blockchain are un set de două chei. O cheie privată, care este utilizată pentru a crea o semnătură digitală pentru o tranzacție, și o cheie publică, cunoscută de toată lumea din rețea. O cheie publică are două utilizări: 1) servește ca adresă în rețeaua blockchain; și 2) este utilizată pentru a verifica o semnătură digitală / pentru a valida identitatea expeditorului. (5)

Pe blockchain-ul Bitcoin, acest lucru se traduce în următorul exemplu. Să presupunem că Anna dorește să îi trimită 100 de bitcoini lui Jeff, atunci mai întâi de toate va trebui să semneze digital această tranzacție folosind cheia sa privată (care este cunoscută doar de ea). Va trebui să adreseze tranzacția către cheia publică a lui Jeff, care este adresa lui Jeff din rețeaua Bitcoin. Apoi, tranzacția, care va fi colectată într-un „bloc de tranzacții”, va trebui verificată de către nodurile din rețeaua Bitcoin. Aici, cheia publică a Anei va fi utilizată pentru a-i verifica semnătura. Dacă

semnătura Anna este validă, rețeaua va procesa tranzacția, va adăuga blocul în lanț și va transfera 100 de bitcoini de la Anna la Jeff.

Cheile publice și private ale unui utilizator sunt păstrate într-un portofel digital sau portofel electronic. Un astfel de portofel poate fi stocat sau salvat online (stocarea online este adesea denumită „stocare la cald”) și / sau offline (stocarea offline este denumită în mod obișnuit „stocare la rece”). (6)

Unul dintre avantajele cheie ale tehnologiei blockchain este că permite simplificarea executării unei game largi de tranzacții care ar necesita în mod normal intermedierea unui terț (de exemplu, un custode, o bancă, un sistem de decontare a valorilor mobiliare, brokeri-dealeri, un depozit de tranzacții, ...). În esență, blockchain se referă la descentralizarea încrederii și la permiterea autentificării descentralizate a tranzacțiilor. (7) Pur și simplu, permite eliminarea „intermediarului”. (8)

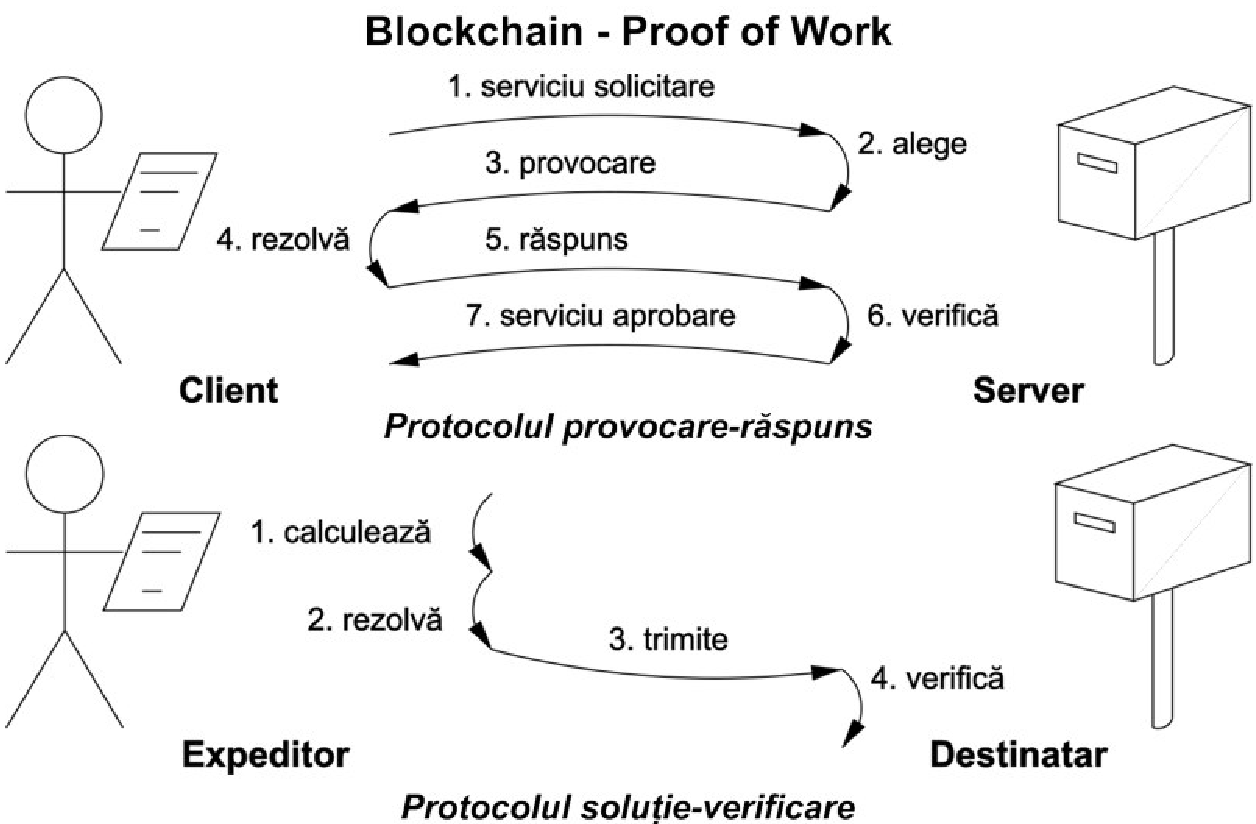
În multe cazuri, acest lucru va duce probabil la creșterea eficienței. Cu toate acestea, este important să subliniem faptul că poate expune părțile care interacționează la anumite riscuri care au fost gestionate anterior de acești intermediari. De exemplu, Banca pentru Decontări Internaționale („BIS”) a avertizat recent într-un raport din 2017 intitulat *Distributed ledger technology in payment, clearing and settlement* (9), că adoptarea tehnologiei blockchain ar putea introduce noi riscuri de lichiditate. (10) Mai mult, în general, se pare că atunci când un intermediar funcționează ca un tampon împotriva riscurilor importante, cum ar fi riscul sistemic, el nu poate fi înlocuit pur și simplu cu tehnologia blockchain.

Mecanismele de consens blockchain

În principiu, orice nod din cadrul unei rețele blockchain poate propune adăugarea de informații noi în blockchain. Pentru a valida dacă această adăugare de informații (de exemplu o înregistrare de tranzacție) este legitimă, nodurile trebuie să ajungă la o formă de acord. Aici intră în joc un „mecanism de consens”. Pe scurt, un mecanism de consens este o metodă de validare specifică (criptografică) predefinită care asigură o secvențiere corectă a tranzacțiilor pe blockchain. (11) În cazul criptomonedelor, o astfel de secvențiere este necesară pentru a aborda problema „dublei cheltuieli” (adică problema că același instrument de plată sau activ poate fi transferat de mai multe ori dacă transferurile nu sunt înregistrate și controlate centralizat (12)).

Un mecanism de consens poate fi structurat în mai multe moduri. În continuare, cele două exemple de mecanisme de consens cele mai cunoscute - și, în contextul criptomonedelor, de asemenea cel mai frecvent utilizate - vor fi discutate pe scurt: mecanismul Proof of Work („PoW”) și mecanismul Proof of Stake („PoS”).

Proof of Work (PoW)



Într-un sistem PoW, participanții la rețea trebuie să rezolve așa-numitele „puzzle-uri criptografice” pentru a li se permite să adauge noi „blocuri” la blockchain. Acest proces de rezolvare a puzzle-urilor este denumit în mod obișnuit „minerit”. (13) În termeni simpli, aceste puzzle-uri criptografice sunt alcătuite din toate informațiile înregistrate anterior pe blockchain și un nou set de tranzacții care trebuie adăugat la următorul „bloc”. (14) Deoarece intrarea fiecărui puzzle devine mai mare în timp (rezultând un calcul mai complex), mecanismul PoW necesită o cantitate mare de resurse de calcul, care consumă o cantitate semnificativă de energie electrică. (15)

Dacă un participant la rețea (adică un nod) rezolvă un puzzle criptografic, dovedește că a finalizat lucrarea și este recompensat cu o formă digitală de valoare (sau, în cazul unei criptomonede, cu o monedă nou minerită). Această recompensă servește drept stimulent pentru susținerea rețelei. (16)

Criptomoneda Bitcoin se bazează pe un mecanism de consens PoW. Alte exemple includ Litecoin, Bitcoin Cash, Monero etc. (17)

Proof of Stake (PoS)

Într-un sistem PoS, un validator de tranzacții (adică un nod de rețea) trebuie să dovedească proprietatea asupra unui anumit activ (sau în cazul criptomonedelor, o anumită cantitate de monede) pentru a participa la validarea tranzacțiilor. Acest act de validare a tranzacțiilor se numește „forjare” (18) în loc de „minerit”. De exemplu, în cazul criptomonedelor, un validator de tranzacții va trebui să-și demonstreze „valoarea financiară” (cota sa) din toate monedele existente pentru a i se permite să valideze o tranzacție. În funcție de câte monede deține, va avea șanse mai mari de a fi cel care va valida următorul bloc (adică totul are legătură cu faptul că are o vechime mai mare în rețea, ceea ce îi conferă o poziție mai de încredere). (19) Validatorul tranzacției primește o taxă de tranzacție pentru serviciile sale de validare de către părțile care efectuează tranzacția. (20)

Criptomonedele precum Neo și Ada (Cardano) utilizează un mecanism de consens PoS (21).

Alte mecanisme

Mecanismele PoW și PoS sunt departe cele mai folosite mecanisme de consens existente în prezent. (22) Alte exemple includ ”proof of service”, ”proof of elapsed time” și ”proof of capacity”.

Sursa: Sfetcu, Nicolae (2022). *Criptomonede*, MultiMedia Publishing, ISBN 978-606-033-645-7, https://www.telework.ro/ro/e-books/criptomonede/

Bibliografie

(1) Grupul Băncii Mondiale (H. NATARAJAN, S. KRAUSE și H. GRADSTEIN), „Distributed Ledger Technology (DLT) and blockchain”, 2017, nota FinTech, nr. 1. Washington, D.C.,

http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1.

(2) Ibidem, 1. A se vedea, de asemenea, mai jos 2.1.3. Mecanismele de consens blockchain.

(3) CPMI, „Digital currencies”, noiembrie 2015, https://www.bis.org/cpmi/publ/d137.pdf, 5.

(4) A se vedea: Grupul Băncii Mondiale (H. NATARAJAN, S. KRAUSE și H. GRADSTEIN), „Distributed Ledger Technology (DLT) and blockchain”, 2017, nota FinTech, nr. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1.

(5) Ibidem, 8-9.

(6) Inter alia: BCE, „Virtual Currency Schemes – a further analysis”, februarie 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8; FATF, „Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, iunie 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential -aml-cft-riscuri.pdf, 8.

(7) P. WITZIG și V. SALOMON, „Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry”, Document de lucru 1, 2018 / E, Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 5.

(8) Trebuie remarcat faptul că pe blockchain-urile permise există încă un rol pentruo parte centrală (a se vedea și mai sus).

(9) CPMI, „Distributed ledger technology in payment, clearing and settlement – An analytical framework”, februarie 2017, https://www.bis.org/cpmi/publ/d157.pdf.

(10) Ibidem, 19.

(11) A se vedea: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “*Distributed Ledger Technology (DLT) and blockchain*”, 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 6.

(12) R. HOUBEN, „Bitcoin: there two sides to every coin”, ICCLR, Vol. 26, numărul 5, 2015, 195.

(13) A se vedea: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), “*Distributed Ledger Technology (DLT) and blockchain*”, 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 6.

(14) EY, „*IFRS - Accounting for crypto-assets*”, martie 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 17.

(15) De exemplu, consumul anual actual de energie electrică Bitcoin (unul dintre cele mai cunoscute exemple de criptomonedă bazat pe un mecanism PoW) este echivalent cu consumul anual de energie electrică consumat în Republica Cehă. Printre altele: https://digiconomist.net/bitcoin-energy-consumption; S. LEE, „*Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That'*”, aprilie

2018, https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/.

(16) World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "*Distributed Ledger Technology (DLT) and blockchain*", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 6

(17) A se vedea, de asemenea, Bitcoin și nu numai: cele 10 criptomonede cu cea mai mare capitalizare de piață din acest ghid.

(18) Un nod „forjează" fiecare bloc. A se vedea: EY, "*IFRS – Accounting for crypto-assets*", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 17.

(19) EY, "*IFRS – Accounting for crypto-assets"*, March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 17.

(20) În principiu, criptomonedele care utilizează un mecanism PoS sunt deja pre-minate. Prin urmare, forjarea nu creează monede noi. Vezi: ibid.

(21) Trebuie remarcat faptul că criptomoneda Ethereum este un caz special. Ethereum s-a bazat pe un mecanism PoW de la început, dar comunitatea sa de dezvoltatori intenționează acum să actualizeze acel mecanism și să îl suprapună cu un mecanism PoS. Vezi de exemplu:: S. JAGATI, "*Ethereum's Proof of Stake Protocol Under Review*", April 2018, https://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/.

(22) A se vedea, de asemenea: Ibid.